Express5800/FW300a、Express5800/FW500b に添付される Check Point CD-ROM が『 **NG FP3** 』から『 **NG with Application Intelligence** 』に変更されることに伴い、ユーザーズガイドの差し替えを行います。
以下に記述する FireWall-1のコンフィグレーション、インストール箇所に関しては、本ドキュメントの記述を参照し、実施してください。

３．システムのセットアップ

セットアップ

２．　システムのセットアップ

FireWall-1のコンフィグレーション　(※1)

３．　セキュリティポリシーのセットアップ

GUIクライアントのインストール　(※2)

再セットアップ

システムの再起動

再インストールの準備(SSH接続)（※3)

再インストールの手順　(※4)

４．　二重化構成について

セットアップ

FireWall-1管理サーバのセットアップ

FireWall-1管理モジュールのコンフィグレーション　(※5)

Firewall本体のセットアップ

FireWall-1のコンフィグレーション　(※6)

FireWall-1 のコンフィグレーション（※1）

次に管理コンピュータからFireWall-1 付属のcpconfigコマンドを実行します。
以下の手順でコンフィグレーションを行ってください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...  ……………………………………………… ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y  ……… ②


Select installation type:
-------------------------

(1) Stand Alone - install VPN-1 / FireWall-1 Internet Gateway.
(2) Distributed - select components of the Enterprise Product.

Enter your selection  (1-2/a-abort) [1]: 1  ……………………………… ③
Would you like to enable SecureXL acceleration feature? (y/n) [y] ? n  …… ④
IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your VPN-1 & FireWall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
```

① <Enter>キーを押すと使用許諾書が表示されますのでお読みください。
② 使用許諾に承認した場合は<Y>キーを押す。
③ インストールするモジュールを選択する。
　通常は 1 を選択し、一体型構成でインストールします。
　FireWall-1管理モジュールを別マシンにインストールして管理する、分散型構成でインストールする場合は 2 を選択してください。二重化のために分散型構成でインストールする場合、以降の設定内容については「二重化構成について」を参照してください。
④ SecureXLの使用/未使用を設定する。
　本製品では、SecureXLを使用しませんので、<N>を選択します。

```
Configuring Licenses...
=======================
Host           Expiration Features

Note: The recommended way of managing licenses is using SmartUpdate.
cpconfig can be used to manage local licenses only on this machine.

Do you want to add licenses (y/n) [n] ? y  ……………… ①

Do you want to add licenses [M]anually or [F]etch from file: m  ……… ②
IP Address: 202.247.5.126  ┐
Expiration Date:           │
Signature Key:             │ ……………… ③
SKU/Features:              ┘

License was added successfully

 License will be put into kernel after cpstart


Configuring Administrators...
=============================
No VPN-1 & FireWall-1 Administrators are currently
defined for this SmartCenter Server.

Do you want to add administrators (y/n) [y] ? y  ……………… ④
Administrator name: fws-admin  ┐
Password:                      │ ……………… ⑤
Verify Password:               ┘
Permissions for all products (Read/[W]rite All, [R]ead Only All,
[C]ustomized) w
       Permission to Manage Administrators ([Y]es, [N]o) y

Administrator fws-admin was added successfully and has
Read/Write Permission for all products with Permission to Manage
Administrators

Add another one (y/n) [n] ? n  ……………… ⑥
```

① <Y>キーを入力して、ライセンスを追加する。
② <M>キーを入力して、ライセンスを画面から(マニュアルで)入力する。
③ 事前に取得したライセンス情報を入力する。
ライセンスは、Firewallのライセンス製品に添付されている「ライセンス申請書」をNSSolへFAX して取得してください。本製品には「ライセンス申請書」は含まれていません(「Firewallの製品体系」を参照してください)。
④ <Y>キーを入力して、管理者登録を行う。
⑤ Firewall（FireWall-1）の管理者名、およびパスワード、属性を設定する。
⑥ 管理者を追加する場合は<Y>キーを、登録を終了する場合は<N>キーを押す。

```
Configuring GUI Clients...
==========================
GUI Clients are trusted hosts from which
Administrators are allowed to log on to this SmartCenter Server
using Windows/X-Motif GUI.

No GUI Clients defined
Do you want to add a GUI Client (y/n) [y] ? y ···························· ①

You can add GUI Clients using any of the following formats:
1. IP address.
2. Machine name.
3. "Any" - Any IP without restriction.
4. A range of addresses, for example 1.2.3.4-1.2.3.40
5. Wild cards - for example 1.2.3.* or *.checkpoint.com

Please enter the list of hosts that will be GUI Clients.
Enter GUI Client one per line, terminating with CTRL-D or your EOF
character.
192.168.1.99 ···························· ②
Is this correct (y/n) [y] ? y ···························· ③


Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used in
various cryptographic operations.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

   [....................] ···························· ④

Thank you.
```

① <Y>キーを入力して、クライアントマシンのリストを新規作成する。

② セキュリティポリシーの設定を行うクライアントマシンのIPアドレスを設定する。
複数のIPアドレスを設定する場合は改行して複数行入力する。入力を終了する場合は<Ctrl>-<D>キーを押してください。

③ 入力したアドレスが正しければ<Y>キーを押す。

④ バーがフルになるまでランダムキー入力をする。

```
Configuring Certificate Authority...
====================================

The Internal CA will now be initialized
with the following name: fws.nec.co.jp

Initializing the Internal CA...(may take several minutes)
 Internal Certificate Authority created successfully
 Certificate was created successfully
Certificate Authority initialization ended successfully

Check Point product Trial Period will expire in 15 days.
Until then, you will be able to use the complete Check Point Product
Suite.
Trying to contact Certificate Authority. It might take a while...
fws.nec.co.jp was successfully set to the Internal CA

Done


Configuring Certificate's Fingerprint...
========================================
The following text is the fingerprint of this SmartCenter Server:
ADD OX GAWK MUM LONG RISK CARD FERN LILY KEY JOKE FLOC

Do you want to save it to a file? (y/n) [n] ? n ……… ①
generating INSPECT code for GUI Clients
initial_management:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y ……… ②
```

① GUIクライアントを接続したとき、接続したFireWall-1が正しいものであるかを確認するための文字列が表示される。
この文字列をディスク上に保存する場合は<Y>キーを、保存しない場合は<N>を入力します。

② 終了後、再起動する。
再起動後は、FireWall-1のデフォルトフィルタが有効になるため、SSH、WbMCでの接続が不可となります。

GUIクライアントのインストール（※2）

管理クライアントにSmartDashboardをインストールします。ここでは、SmartDashboardといっしょにログを解析するためのツール「SmartView Tracker」とシステムの状態をチェックする「SmartView Status」もインストールします。

1. コンピュータのCD-ROMドライブにCheck Point Next GenerationのCD-ROMをセットする。
   自動的にインストールプログラムが起動し、画面が表示されます。
   インストールプログラムが起動しない場合は\ｗｒａｐｐｅｒｓ\ｗｉｎｄｏｗｓ フォルダにある「demo32.exe」を実行してください。
   Welcome画面が表示されます。

2. ［Next］をクリックする。
   使用許諾契約書が表示されます。

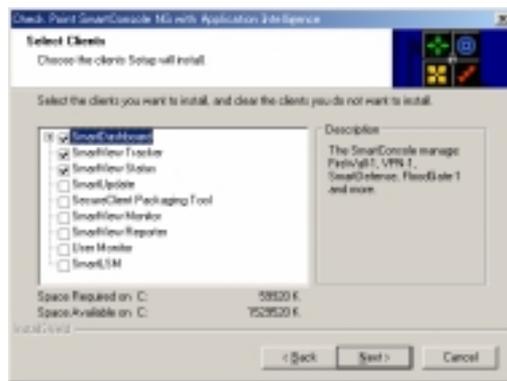
3. 内容をよく読み、同意する場合は［Yes］をクリックする。
   同意しない場合は［No］をクリックして終了します。
   ［Installation Options］画面が表示されます

4. ［New Installation］を選択し、［Next］をクリックする。
   Product選択画面が表示されます。

5. Management Consoleの[SmartConsole]のみにチェックし、[Next]をクリックする。

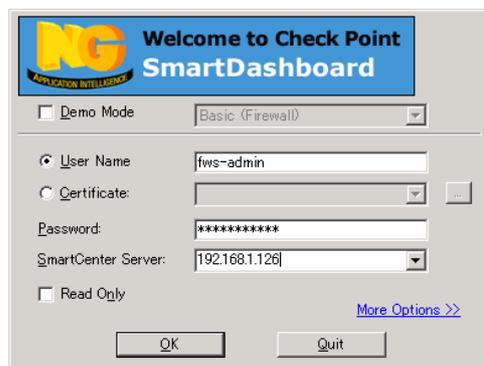
6. インストールするProductsが表示されますので、[SmartConsole]と表示されていることを確認し、[Next]をクリックする。
   Choose Destination Location画面が表示されます。

7. 必要に応じてフォルダを変更し、[Next]をクリックする。
   インストールするコンポーネントを選択する画面が表示されます。

8. [SmartDashboard]、[SmartView Tracker]および[SmartView Status]をチェックし、[Next]をクリックする。
   インストールが開始されます。

9. ショートカット作成を行うかのメッセージが表示される。
   作成する場合は「はい」をクリックします。

10. Setup完了のメッセージが表示されるので、［OK］をクリックする。

11. Informationダイアログが表示されるので、［OK］をクリックする。

12. SmartDashboardを起動し、cpconfig で登録したユーザ名とパスワード、およびFirewallの内側(管理クライアント側)のアドレスを入力する。
    SmartDashboardを使用し、Firewallと接続してポリシーを作成します。ネットワーク構成に応じたポリシールールを作成してください。
    SmartDashboardの使い方、セキュリティポリシーの設定等についてはFireWall-1に付属のマニュアルを参照してください。

再インストールの準備(SSH準備)（※3）

作業を行うためには、SSH接続用管理クライアントが必要です。本体の電源がOFFの状態で、SSH接続用管理クライアントを本体背面のLANポートインタフェース(内部ネットワーク用)にクロスケーブル接続してください。また、Firewallに直接LANケーブルを接続しないで、内部ネットワークに接続する場合は、ハブなどにLANケーブルで接続してください。

Firewallとの接続に必要なもの

- SSH接続用管理クライアント
- LANケーブル

再インストールに必要なディスク

あらかじめ以下のディスクを用意してください。

- バックアップCD-ROM
- Check Point Next Generation(NG with Application Intelligence)
- 再インストール用ディスク
- 初期化導入設定用ディスク
- バックアップディスク(任意)

再インストール手順（※4）

1. 本体の電源をONにし、前面にあるフロッピーディスクドライブに再インストール用ディスクを、CD-ROMドライブにバックアップCD-ROMをセットする。

   自動的にプログラムCD-ROMからのインストールが始まります。

   インストールは約10分で完了します。
   インストールを完了すると、CD-ROMドライブからバックアップCD-ROMが排出されます。
   本体は、電源が入った状態で、システムが停止している状態になります。

2. バックアップCD-ROMおよび再インストール用ディスクを取り出した後、POWERスイッチを押して電源をOFFにする。

3. 初期導入設定用ディスクをセットし、POWERスイッチを押して電源をONにする。
   初期導入設定用ディスクは、初期導入設定用ツールで作成済みのものとします。
   しばらく（3分程度）してから管理クライアントからSSHクライアントにて、Firewallへログインします。

4. 管理クライアントから初期導入設定用ツールで設定したSSHの｢管理者アカウント名｣と｢Password｣を利用し、ログインする。

5. <バックアップしておいた設定をリストアする場合>
   以下のコマンドを実行して設定を行う。
   設定をバックアップしたフロッピーディスクを本体にセットしてください。

```
# fwrestore -i
Please insert backup floppy disk. (#1)
Press enter key.
restore fws.ini ...
restore clp.conf ...
restore .http...
restore .ssh...
restore completed.
After turned off FDD access light, Press enter key.
# fwsetup -i /opt/necfws/etc/fws.ini
       :
       :
# shutdown -r now
```


<バックアップのリストアをしない場合>
本章の「2．システムのセットアップ」-「基本設定ツールによる設定」を参照して設定を行い、終了後、再起動する。

6. 起動後、CD-ROMドライブにCheck Point Next Generation（NG with Application Intelligence）の CD-ROMをセットし、FireWall-1のモジュールを以下の手順で適用する。

```
# mount /dev/cdrom
# cd /mnt/cdrom/linux/
# rpm -i ./CPshared-50/CPshrd-50-04.i386.rpm
# rpm -i ./CPFirewa1ll-50/CPfw1-50-04.i386.rpm
# cd /
# umount /dev/cdrom
```

7. CD-ROMドライブからCD-ROMを取り出し、再起動する。

```
# shutdown -r now
```

8. cpconfigを実行してFireWall-1の設定を行う。
cpconfigについては本章の「2. システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

```
# cpconfig
    :
    :
Do you want to reboot? (y/n) [y] ? y
```

9. ポリシーの作成を行う。
<あらかじめバックアップしておいた設定をリストアする場合>
以下のコマンドを実行してFireWall-1の設定をする。

```
# cpstop
# fwrestore -f
Please insert backup floppy disk. (#1)
Press enter key.
There is 1 floppy disk for restore.
restore fw config files...(1/1)
restore completed.
After turned off FDD access light, Press enter key.
# cpstart
```


<バックアップのリストアをしない場合>
SmartDashboardを使用してポリシーを作成する。

10. SmartDashboardでポリシーをインストールする。

【 重要 】
CD-ROMドライブにCheck Point Next Generation（NG with Application Intelligence）のCD-ROMをセットした状態のままFirewall本体を起動しないように注意してください。

FireWall-1 管理サーバのセットアップ

FireWall-1管理モジュールのコンフィグレーション（※5）

管理モジュールを管理サーバへインストールします。以下の手順でコンフィグレーションを行ってください。図中の〈略〉の設定する項目については、3章の「2. システムのセットアップ」-「FirewWall-1のコンフィグレーション」を参照してください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...                                             ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y        ②


Select installation type:
-------------------------

(1) Stand Alone - install VPN-1 / FireWall-1 Internet Gateway.
(2) Distributed - select components of the Enterprise Product.

Enter your selection  (1-2/a-abort) [1]: 2                             ③


Select installation type:
-------------------------

(1) Enforcement Module.
(2) Enterprise SmartCenter.
(3) Enterprise SmartCenter and Enforcement Module.
(4) Enterprise Log Server.
(5) Enforcement Module and Enterprise Log Server.

Enter your selection  (1-5/a-abort) [1]: 2                             ④
```

① FireWall-1管理モジュールのコンフィグレーションをする。
② 使用許諾に承認した場合は<Y>キーを押す。
③ インストールするモジュールを選択する。
　二重化構成の場合は「2」を選択し、インストールします。
④ インストールするモジュールを選択する。
「2」を選択し、管理モジュールをインストールします。

```
Please select SmartCenter type:
------------------------------

(1) Enterprise Primary SmartCenter.
(2) Enterprise Secondary SmartCenter.

Enter your selection  (1-2/a-abort) [1]: 1 ............................ ①
This program will guide you through several steps where you
will define your SVN Foundation configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
           :
          (略)
           :
************* Installation completed successfully *************

Do you wish to start the installed product(s) now? (y/n) [y] ? y ...... ②
cpstart: Power-Up self tests passed successfully
           :
          (略)
           :
FireWall-1: This is a Management Station. No security policy will be loaded
FireWall-1 started

# shutdown -r now ...................................................... ③
```

⑦　インストールする管理モジュールのタイプを選択する。
　　「1」を選択し、Primaryとして使用します。
⑧　管理モジュールを起動させる。
⑨　再起動する。

Firewall本体のセットアップ

FireWall-1のコンフィグレーション（※5）

二重化構成の場合、コンフィグレーション手順が3章とは一部異なります。図中の〈略〉の設定する項目については、3章の「2．システムのセットアップ」-「FireWall-1のコンフィグレーション」を参照してください。

```
# cpconfig


Welcome to Check Point Configuration Program
=================================================
Please read the following license agreement.
Hit 'ENTER' to continue...  ..................................... ①
                :
                :
                :
Do you accept all the terms of this license agreement (y/n) ? y ...... ②


Select installation type:
-------------------------

(1) Stand Alone - install VPN-1 / FireWall-1 Internet Gateway.
(2) Distributed - select components of the Enterprise Product.

Enter your selection  (1-2/a-abort) [1]: 2 ............................ ③


Select installation type:
-------------------------

(1) Enforcement Module.
(2) Enterprise SmartCenter.
(3) Enterprise SmartCenter and Enforcement Module.
(4) Enterprise Log Server.
(5) Enforcement Module and Enterprise Log Server.

Enter your selection  (1-5/a-abort) [1]: 1 ............................ ④
```

① FireWall-1管理モジュールのコンフィグレーションをする。
② 使用許諾に承認した場合は<Y>キーを押す。
③ インストールするモジュールを選択する。
二重化構成の場合は「2」を選択し、インストールします。
④ インストールするモジュールを選択する。
二重化構成の場合は「1」を選択し、インストールします。

```
Is this a Dynamically Assigned IP Address Module installation ? (y/n) [n] ?  ①
Would you like to install a Check Point clustering product (CPHA, CPLS or State
Synchronization)? (y/n) [n] ? y  ②
Would you like to enable SecureXL acceleration feature? (y/n) [y] ? n  ③
IP forwarding disabled
Hardening OS Security: IP forwarding will be disabled during boot.
Generating default filter
Default Filter installed
Hardening OS Security: Default Filter will be applied during boot.
This program will guide you through several steps where you
will define your VPN-1 & FireWall-1 configuration.
At any later time, you can reconfigure these parameters by
running cpconfig
                              :
                             (略)
                              :
```

③ Dynamically Assigned IP Address Moduleをインストールするか問い合わせがあるので、<Enter>キーを選択する。

④ Check Point clustering productをインストールするか問い合わせがあるので、<Y>キーを押す。

⑤ SecureXLを有効にするかの設定をする。
SecureXLを使用しないので<N>を選択します。

```
                              :
                             (略)
                              :
Configuring Secure Internal Communication...
============================================
The Secure Internal Communication is used for authentication between
Check Point components

Trust State: Uninitialized ┐
Enter Activation Key:      │  ①
Again Activation Key:      ┘

The Secure Internal Communication was successfully initialized

initial_module:
Compiled OK.

Hardening OS Security: Initial policy will be applied
until the first policy is installed


In order to complete the installation
you must reboot the machine.
Do you want to reboot? (y/n) [y] ? y  ②
```

① FireWall-1管理サーバとFirewall間での通信に使用するパスワードを設定してください。

② 終了後、再起動します。